Sistem za Detekciju i Reakciju na Pretnje Informacione Bezbednosti

Članovi Tima:

- Aleksandra Balažević SV37/2020
- Marko Pejanović SV66/2020

Motivacija:

U dobu digitalizacije, sajber pretnje su sveprisutne i neprestano se razvijaju. Postaje sve složenije zaštiti organizaciju od napada. Sistemi za detekciju i odgovor pretnjama postaju ključni za zaštitu organizacija. Ova dinamika stvara pritisak na IT i bezbednosne timove, koji se često suočavaju sa preopterećenjem usled konstantne potrebe za nadzorom i intervencijom. Dodatno, tradicionalni pristupi bezbednosti postaju nedovoljni jer napadači neprestano razvijaju nove metode za zaobilaženje sigurnosnih mera. Rađa se potreba za automatizovanim sistemom za reagovanje na napade.

Pregled problema:

Naš automatizovan sistem omogućavaju brzo i efikasno reagovanje na napade u realnom vremenu i time smanjuju štetu i sprečavaju napade pre nego što izazovu ozbiljne. Ova automatizacija ne samo da ubrzava odgovor na pretnje, već i smanjuje opterećenje na IT i bezbednosne timove, omogućavajući im da se fokusiraju na druge zadatke.

Iako već postoje napredni sistemi za upravljanje informacionom bezbednošću - SIEM (Security Information and Event Management) i EDR (Endpoint Detection and Response), imaju značajnu manu koje naš sistem ima za cilj da reši: **manuelni nadzor i intervencije**. Većina postojećih sistema zahteva određeni stepen manuelnog nadzora i intervencija, što može dovesti do kašnjenja u otkrivanju i reagovanju na pretnje. Na primer, iako SIEM sistemi

mogu automatski da loguju i analiziraju sigurnosne podatke, često je potrebno da ljudski operateri preduzmu akciju na osnovu uzbuna koje sistem generiše.

Metodologija rada:

Očekivani ulazi u sistem:

Glavni ulazi u naš sistem su različite vrste logova. Svaki tip loga ima jedinstvenu svrhu u kontekstu sajber bezbednosti:

- **Sigurnosni logovi:**
    1. Sa mrežnih uređaja kao što su firewall-ovi i ruteri.
    2. Sa sigurnosnih aplikacija, uključujući antivirusne programe i sisteme za detekciju i prevenciju upada (IDS/IPS).
- **Logovi mrežnog saobraćaja:**
    - Logovi koji pokazuju obim prenosa podataka, vreme povezivanja i potencijalne neautorizovane pokušaje pristupa.
    - Logovi koji opisuju neobične obrasce saobraćaja, kao što su iznenadni porasti prenosa podataka ili neobične odlazne veze.
- **Sistemski logovi:**
    1. Logovi operativnog sistema koji opisuju greške i promene stanja sistema.
    2. Aplikacijski logovi koji pružaju uvid u ponašanje, operacije i greške aplikacija.
- **Logovi aktivnosti korisnika:**
    1. Logovi koji beleže aktivnosti korisnika unutar sistema. Korisni su za otkrivanje potencijalnih unutrašnjih pretnji ili neautorizovanih pokušaja pristupa.
    2. Logovi autentifikacije koji detaljišu pokušaje prijave korisnika, uspehe i neuspehe.

Očekivani izlazi iz sistema:

- **Alarmi i obaveštenja:**

  Sistem automatski generiše alarme kada detektuje aktivnosti koje odgovaraju definisanim kriterijumima za pretnje. Svaki alarm sadrži informacije o vrsti pretnje, njenom izvoru, vremenu detekcije, i potencijalnom uticaju na infrastrukturu. Alarmi se direktno šalju adminima.

- **Preporuke za mitigaciju:**

  Uz svaki alarm, sistem pruža specifične preporuke za akcije koje treba preduzeti kako bi se ublažio rizik ili eliminisala pretnja.

Baza znanja:

Na osnovu tipova logova koji ulaze u vaš sistem, različite vrste pretnji mogu biti detektovane našim sistemom.

Detektovane pretnje:

Osnovna pravila:

- Ako se u sadržaju loga pojavljuju reči kao što su: execute,install,setup alarmiraj admina da je to mogući napad Trojanskim virusom
- Ako isti izvor promeni ip adresu korišćenja treba proveriti da li je to mogući napad MITM i alarmirati admina
- Ako se u sadržaju loga pojavljuju reči kao što su: javascript,<script> alarmiraj admina da je to mogući napad Trojanskim virusom
- Ako primetimo da log dolazi od izvora koji ima skoro isti naziv kao neki od izvora u sistemu alarmirati admina da je to mogući pokušaj phishing-a

- Ako primetimo pokušaje neautorizovanih promena u zavisnostima aplikacije, to može ukazivati na pokušaje Dependency Injection, alarmirati admina
- Ako se u sadržaju loga pojavljuju karakteristični SQL termini kao što su "SELECT", "DROP", "INSERT", zajedno sa karakterima kao što su "'" ili "` " ili ";", alarmirajte admina da je to mogući SQL Injection napad.
- Ako korisnik pokušava pristup sistemu izvan uobičajenih radnih sati ili sa geografskih lokacija koje nisu tipične za tog korisnika, alarmirajte admina o mogućem kompromitovanju naloga.
- Ako se u sistemskim logovima pojave izvještaji o iznenadnom ili neobičnom povećanju upotrebe CPU-a, memorije ili diska, koje nije izazvano poznatim i legitimnim procesima, to može ukazivati na prisustvo malvera ili neautorizovane aktivnosti.

CEP:

- Ukoliko sistem primi više od 50 logova od istog izvora za 10 sekundi alarmiraj admina da je potencijalni DOS napad u toku
- Ukoliko ne dobijemo sistemski log od nekog od naših izvora duže od 2 dana, alarmiraj admina proveriti da li je sistem u kvaru
- Ako se detektuje veliki broj zahteva za različite porte sa iste IP adrese u kratkom vremenskom periodu, to može ukazivati na pokušaj skeniranja porta. Alarmirajte admina o potencijalnom pretraživanju mreže od strane napadača.
- Ako se u logovima pojavi iznenadno i značajno povećanje mrežnog saobraćaja koje nije u skladu sa uobičajenim obrascem, alarmirajte admina o mogućem data breach-u ili DDoS napadu.

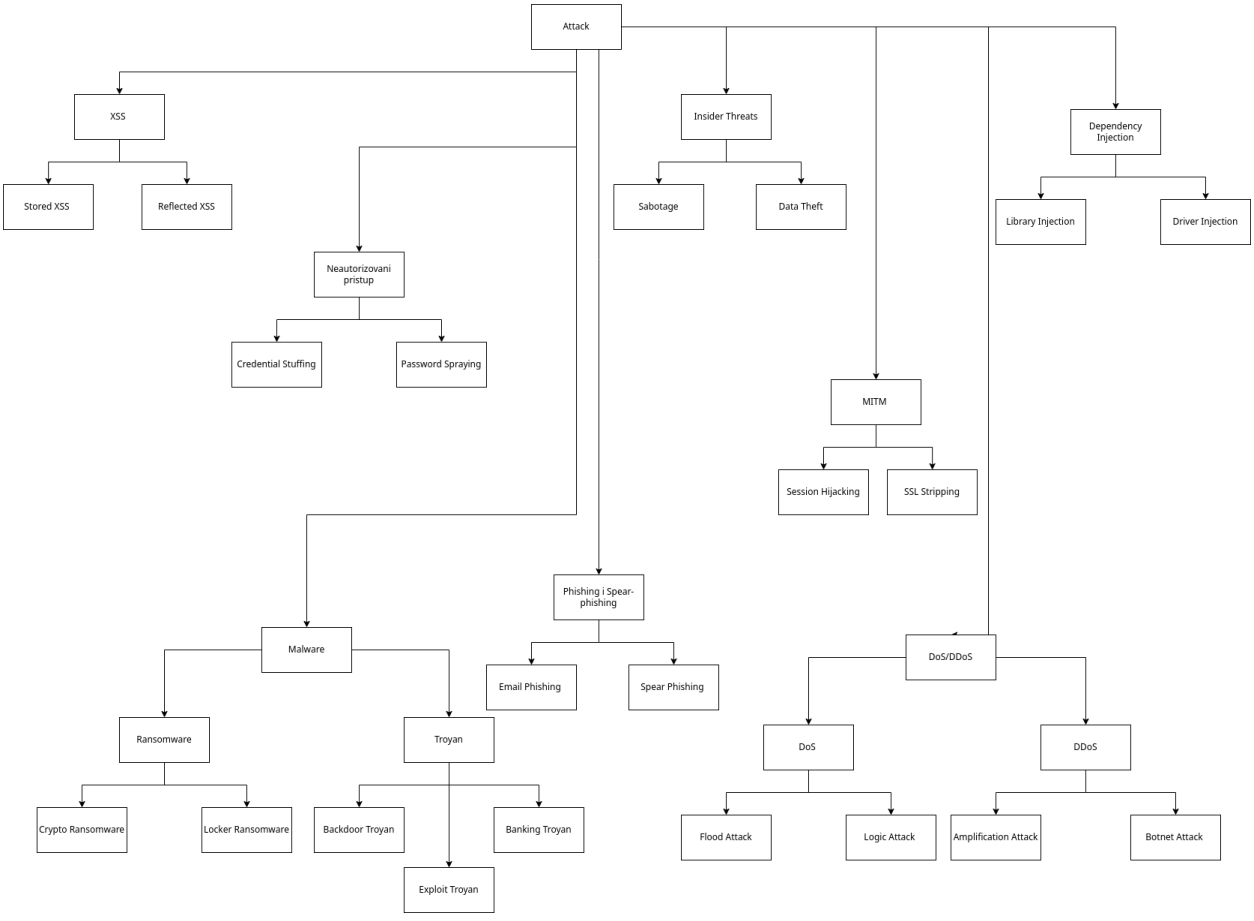
Forward-chaining:

- Detekcija sumnjivih prijava
    - Ako logovi autentifikacije pokazuju neuspešne pokušaje prijave sa iste IP adrese više od 5 puta u 10 minuta, onda izoluj te logove I označi ih kao potencijalno oopasne
    - Ako logovi su označeni kao potencijalno opasni, onda proveri geografsku lokaciju IP adrese .
    - Ako geografska lokacija odgovara poznatim rizičnim zemljama ili neobičnim lokacijama za datog korisnika,Onda označi log kao indikator mogućeg neautorizovanog pristupa.
    - Ako log je označen kao indikator mogućeg neautorizovanog pristupa,Onda pregledaj druge relevantne logove (npr. Logove pristupa sistemima, izmene fajlova) za bilo kakve neobične aktivnosti koje bi mogle biti povezane.

- Ako dodatna analiza logova potvrdi neobičnu ili sumnjivu aktivnost,Onda automatski obavesti sigurnosni tim I blokiraj dalji pristup sa te IP adrese.

- Detekcija sumnjivih logova
  - Ako logovi antivirusnih ili sigurnosnih aplikacija detektuju pokušaj kreiranja ili modifikacije datoteka koje sadrže poznate malver šablone ili čudne ekstenzije, onda označi te datoteke kao potencijalno maliciozne.
  - Ako datoteka je označena kao potencijalno maliciozna, onda analiziraj njeno ponašanje.
  - Ako analiza ponašanja ili statička analiza ukazuju na sumnjivo ponašanje, onda klasifikuj je kao malicioznu.
  - Ako datoteka je klasifikovana kao maliciozna, onda obavesti admine da datoteka treba da se obriše.

Backward-chaining:



- Prilikom dijagnostike tipa napada,razmotriti sve potkategorije napada da bismo utvrdili koji se najbolje uklapa.

Izvestaji:

- Izveštaj o ucestalosti napada iz izabrane kategorije u protekloj jedinici vremena. (Ujedno i template)

Templates:

- Ako se u sadržaju loga pojavljuju ključne reči povezane s poznatim metodama napada (npr. "SQL Injection", "Phishing"), generiši alarm i preporuke za mitigaciju specifične za ovu vrstu pretnje.

- Sistemski logovi pokazuju pokušaje enkripcije ili izmenu velikog broja fajlova u kratkom vremenskom periodu, ili prisustvo poznatih zlonamernih ekstenzija fajlova, ondan generiši alarm i preporuke za mitigaciju specifične za ovu vrstu pretnje.

Diagram klasa: